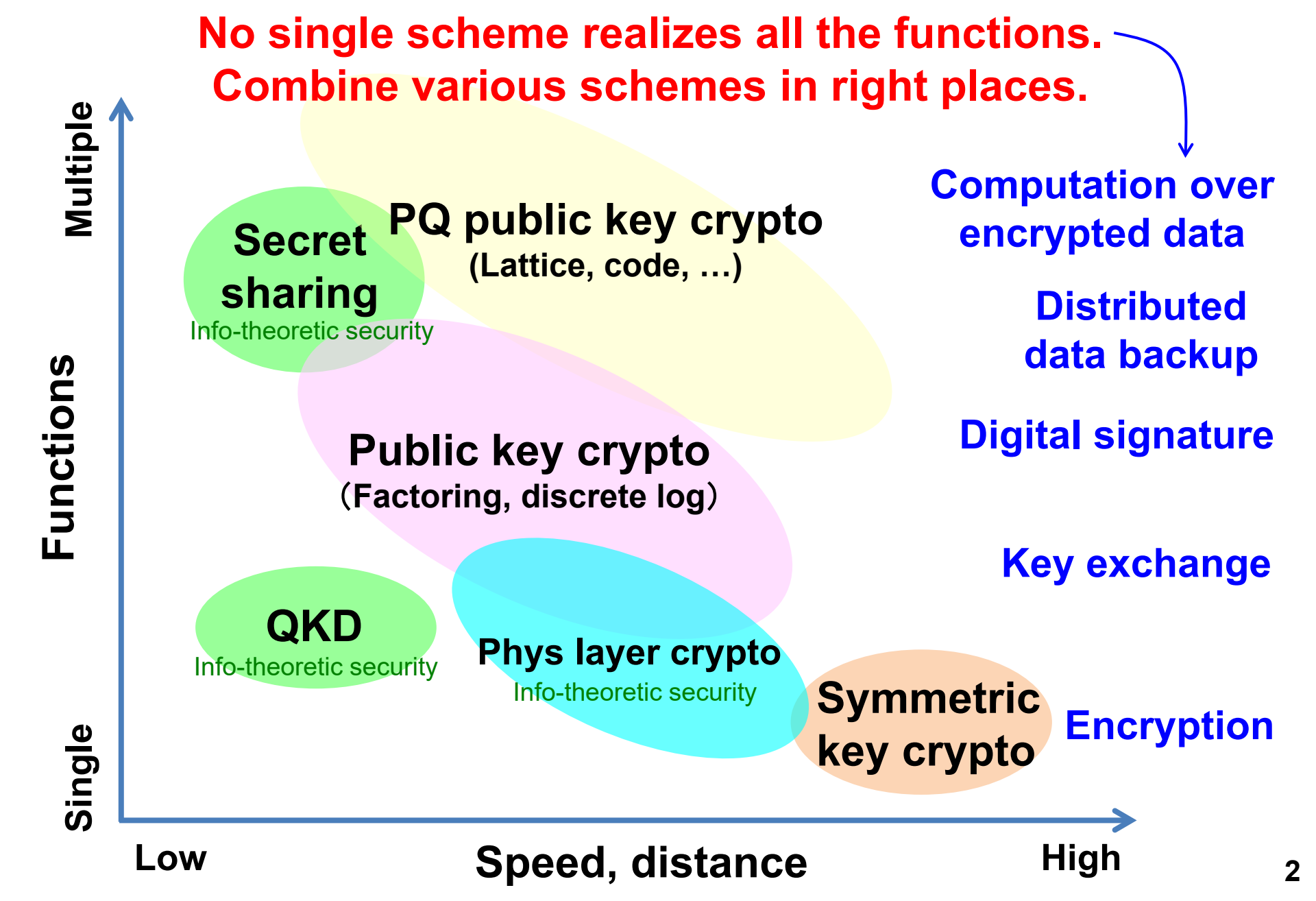
Integration of quantum safe cryptographic technologies

Masahide Sasaki
Director General
Quantum ICT Collaboration Center

Cryptographic technologies

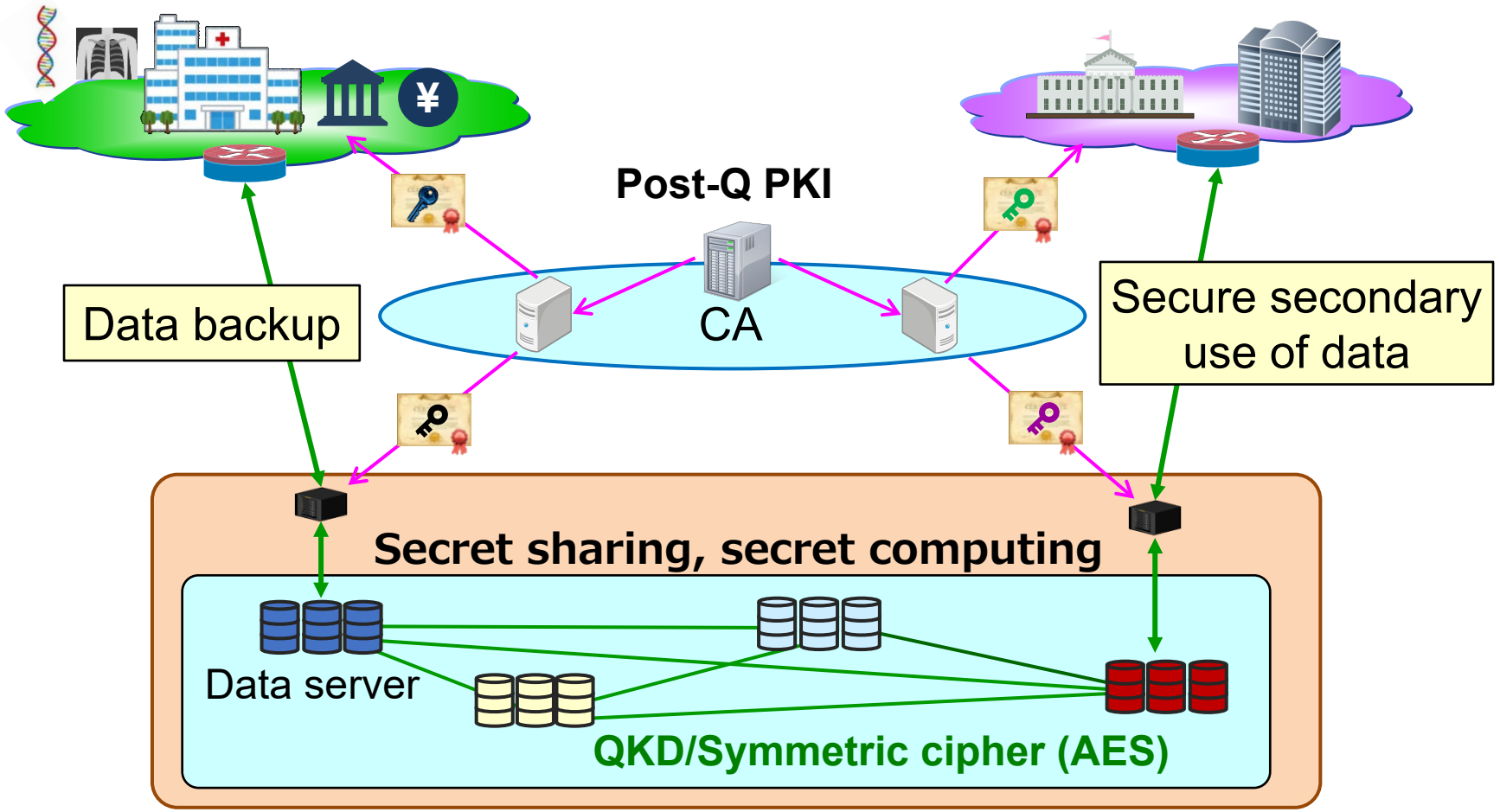


Quantum secure cloud

QKD x Secret sharing → ✓ **Long-term secure data backup**
Availability of data even under disaster

+ Post-Q public key cryptography → ✓ **Secure authentication**

+ Secret computing → ✓ **Secure secondary use of data**



Distributed storage of medical records

(90GB data of 10,000 patients)

Press release (Dec 2019)

https://www.nict.go.jp/en/press/2019/12/12-1.html

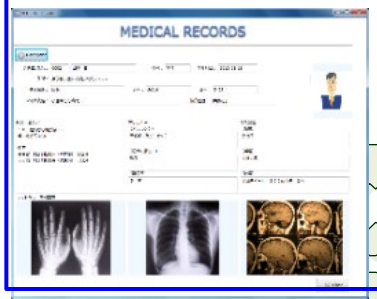
NICT

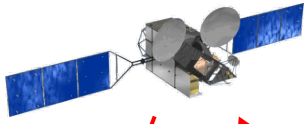
TECHNISCHE UNIVERSITÄT DARMSTADT

ISARA

Kochi Health Science Center

Medical records





We could retore high priority items of patient data (1MB) within 9 sec via a satellite link in an emergency mode.

Osaka

Koganei

Otemachi

Nagoya

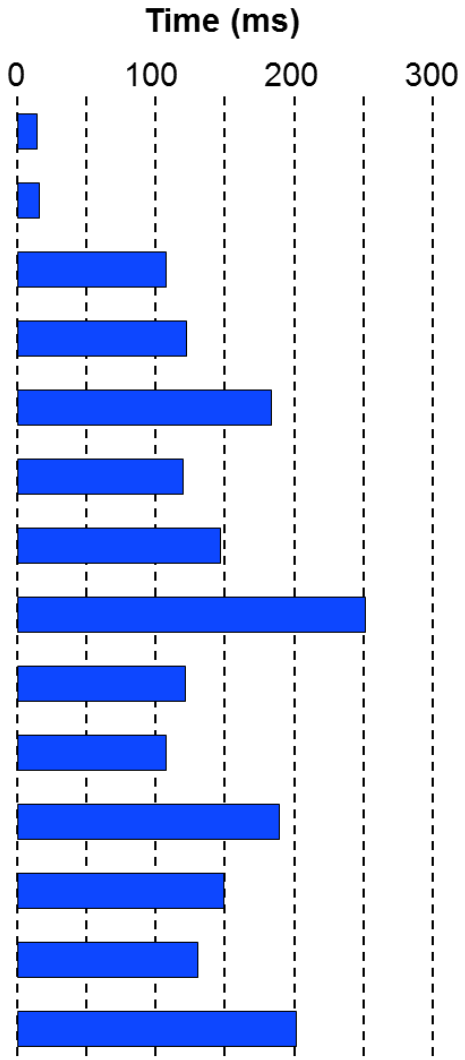
Post-Q VPN

QKD

Totally 800km range

Access control by Post-Q public key authentication

	Root certificate	Key exchange	Signature	Time (ms)
TLS	RSA	ECDHE	SHA384	14.4
		RSA	SHA384	15.8
Post Quantum TLS	LMS (Hash)	NewHope (Lattice)	Dilithum (Lattice)	107.2
			q-TESLA (Lattice)	122.2
			Rainbow (Multivariate)	183.9
		SIDH (Isogeny)	Dilithum (Lattice)	120.2
			q-TESLA (Lattice)	146.4
			Rainbow (Multivariate)	251.7
	XMSS (Hash)	NewHope (Lattice)	Dilithum (Lattice)	121.7
			q-TESLA (Lattice)	107.7
			Rainbow (Multivariate)	189.6
		SIDH (Isogeny)	Dilithum (Lattice)	149.2
			q-TESLA (Lattice)	130.0
			Rainbow (Multivariate)	201.9



12 Post-Q-TLS cipher suites were implemented, and all worked well.
Post-Q-TLS took about 10 times longer processing time as conventional TLS.

Cross referencing between two hospitals with access control by Biometrics + Post-Q signature + ID & password

NEC、NICT、ZenmuTech

Press release (Nov 2020)
https://www.nict.go.jp/en/press/2020/11/20-1.html

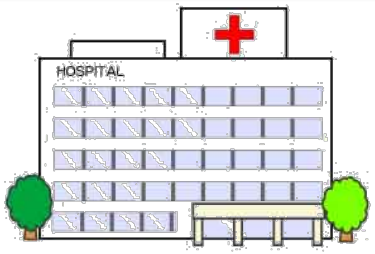
Kochi Health Science Center

Medical records

Standardized data format
SS-MIX

- Standard Storage Root Folder
  - Patient ID: upper 3 digit
    - Patient ID: lower 3 digit
      - Patient ID
        - Examination date
          - Type of Data
            - Patient Data

Hospital in Tokyo

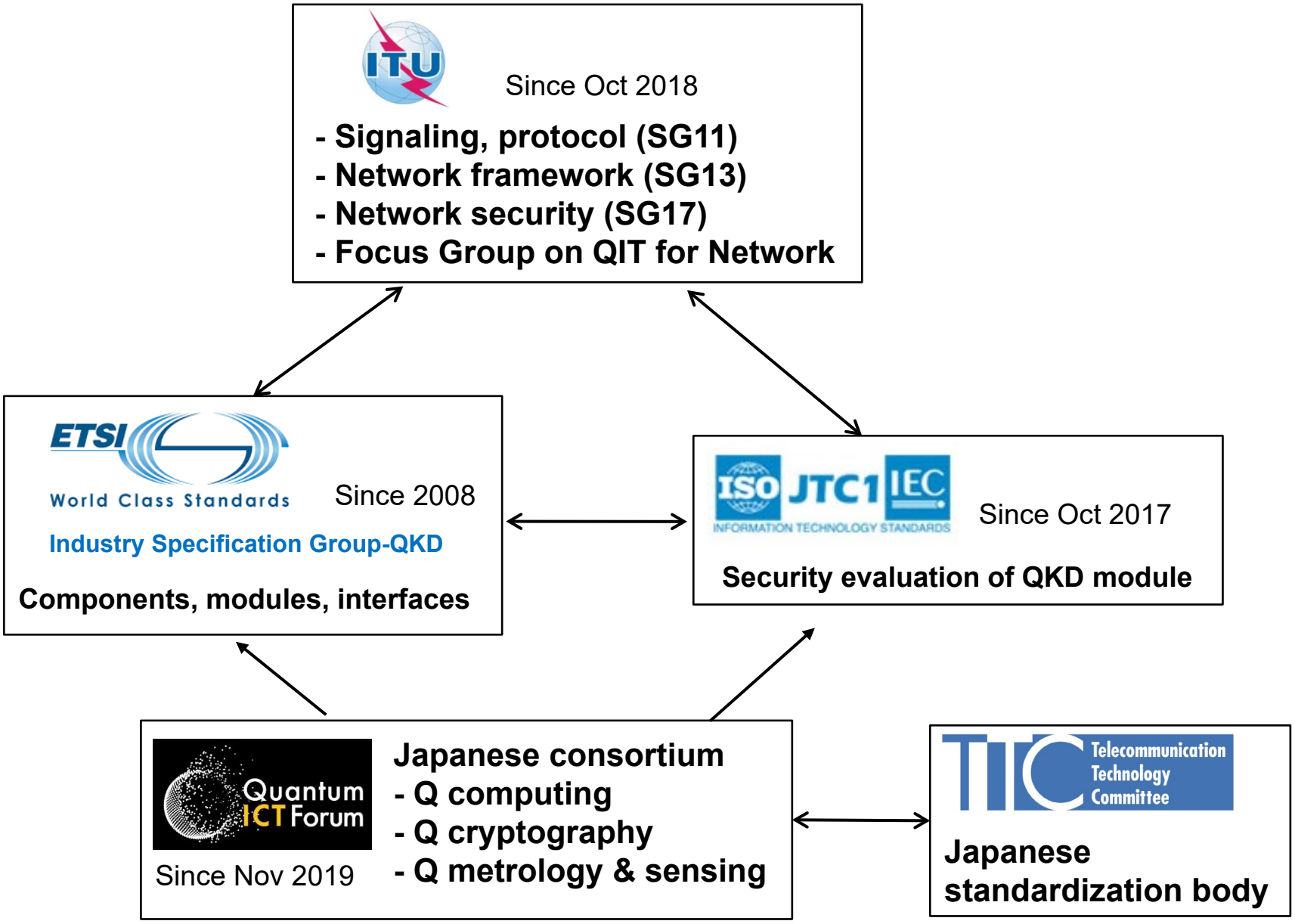


Osaka
Koganei
Nagoya
Otemachi

Q safe-VPN
QKD

Standardization

Standardization activities on QKD



Standardization (QKD network)

Examples of published recommendations and on-going drafts on QKD networks.

Study Group 13 (Network)

Y.3800 Overview of QKDN

Y.3801 NW requirements

Y.3802 NW architecture

Y.3803 Key management

Y.3804 NW control & management

Study Group 17 (Security)

X.1710 Security framework

X.1714 Key combination and supply

Published

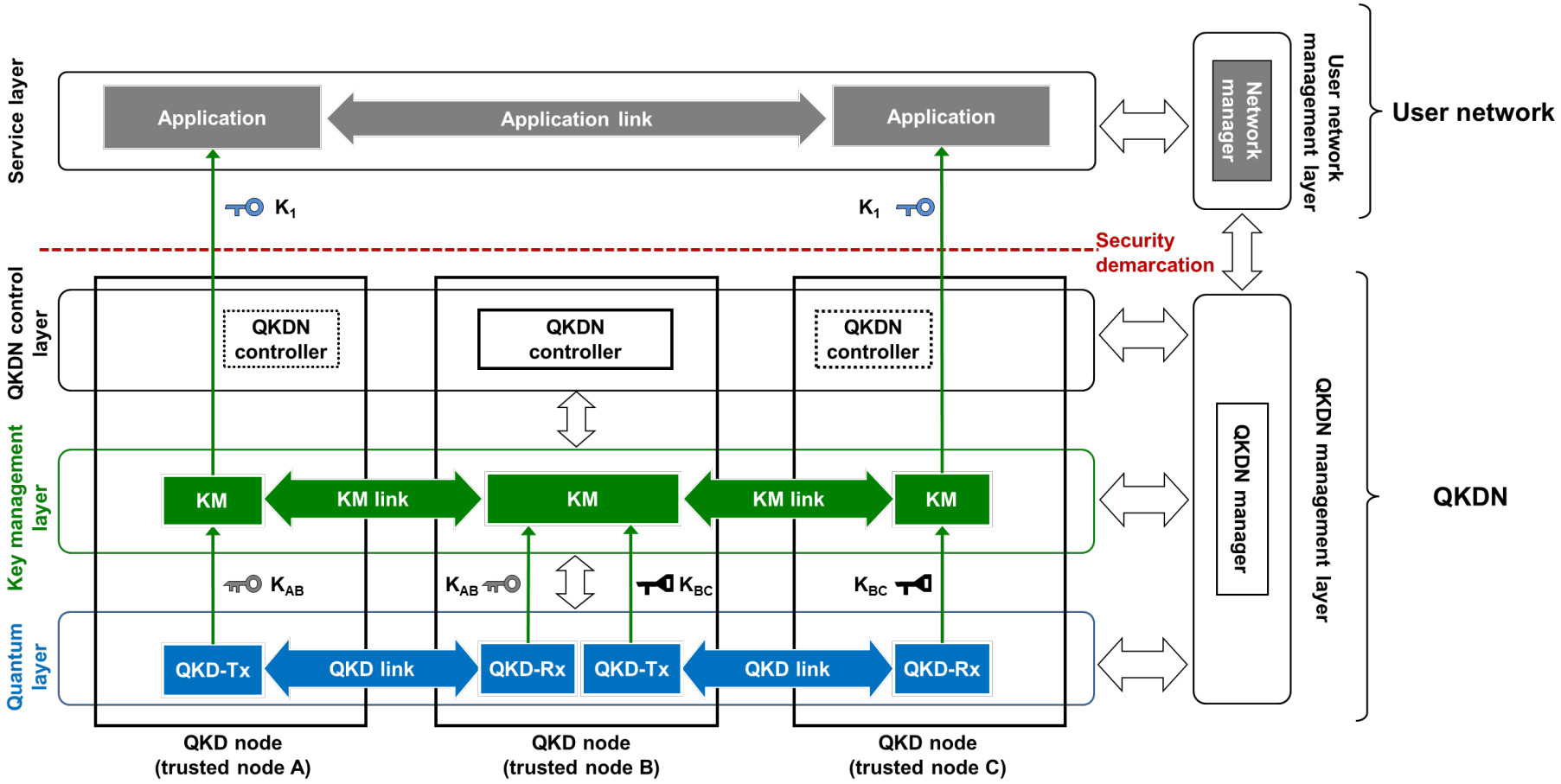
Y.QKDN_frint Secure storage NW

X.sec_QKDN_intrq Requirements for secure storage NW

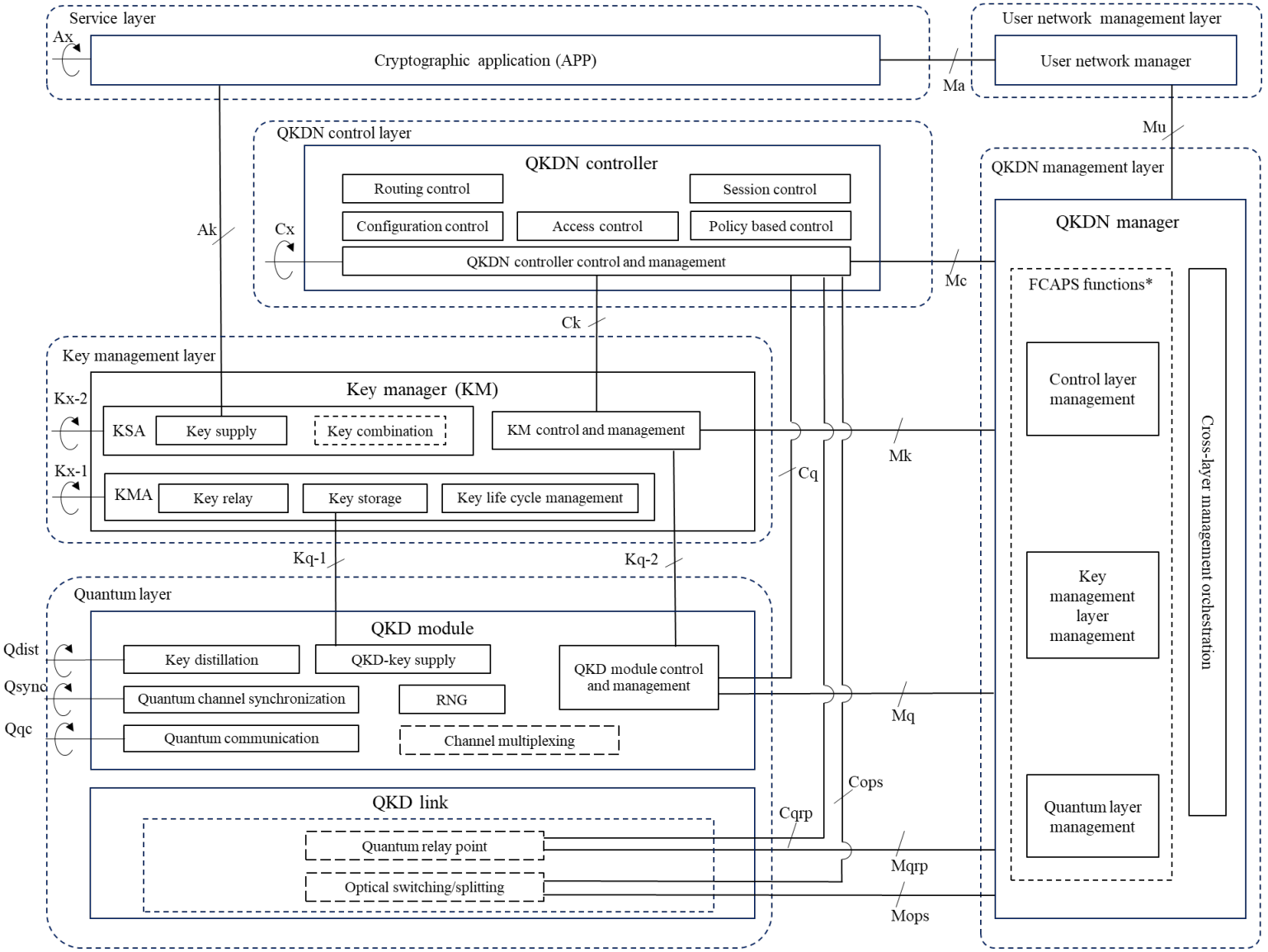
Developing

Y.3800

Overview on networks supporting quantum key distribution

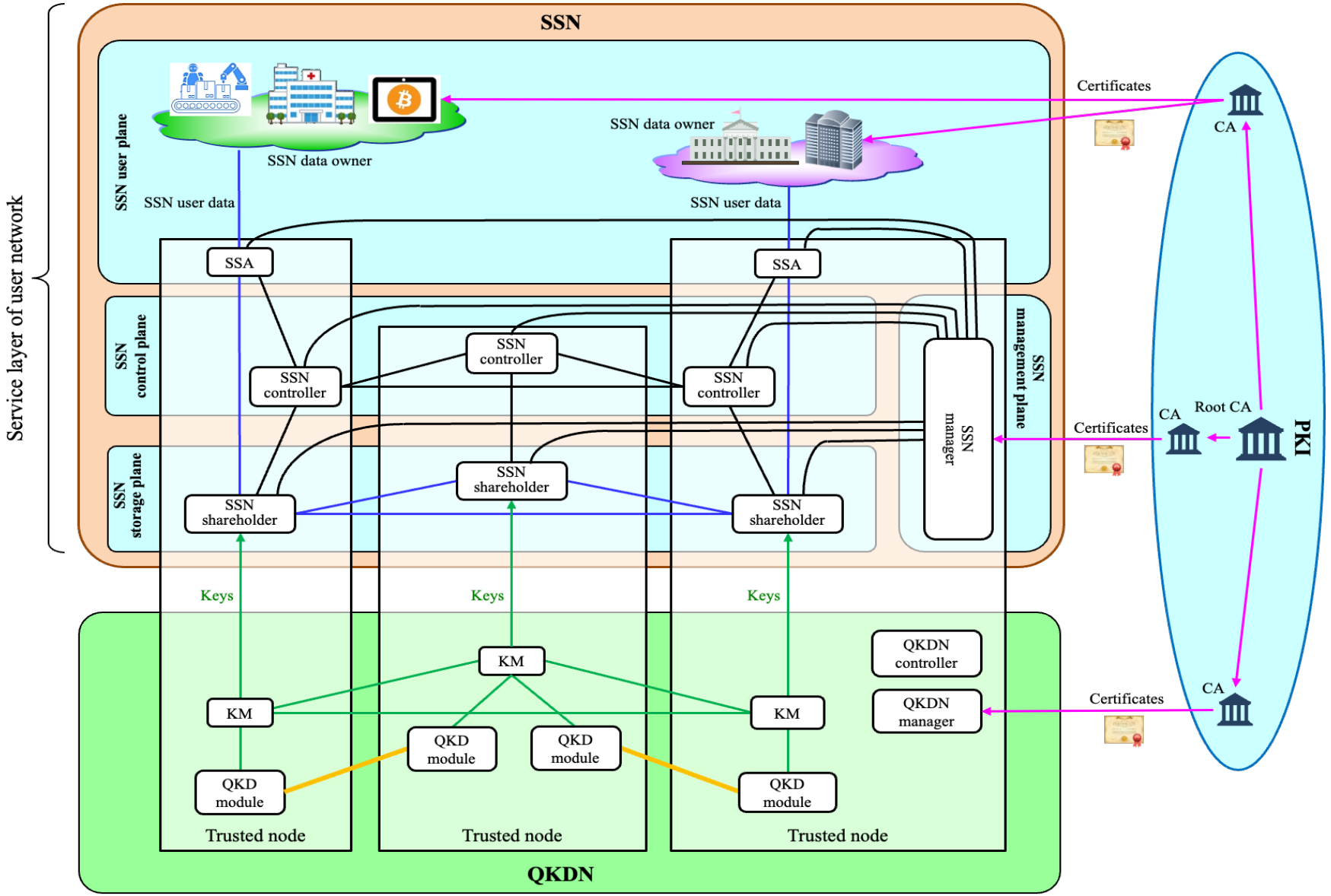


Y.3802
QKD network architecture

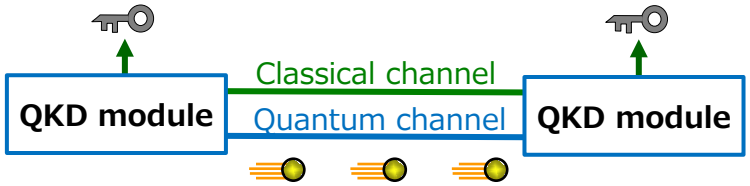


SG13 Y.QKDN_frint

Framework for integration of QKDN and secure storage network



Standardization (QKD module)



ISO/IEC: **Common Criteria** — Developing

Security functional and assurance requirements

Oct 2022

Certification bodies (ETSI, etc): **Protection Profile** — Developing

Generic security evaluation criteria

Government sector version (EAL4+), Sep 2021
Consumer sector version (EAL2), Sep 2022

Evaluation and certification by testing laboratories

Test services in 2023

Product vendors: **Security Target**

Security evaluation criteria for the given product

Suppliers procure certified products

Thank you for your attention